



Safe on Social

Vault apps

Cheat Sheet

Vault Apps

My child has two calculators on their phone?

No, they don't. What they have is one calculator and one vault app.

Vault apps have been in existence for a while now, but with the gradual increase of parents with some social media know-how, they are appearing with regularity on smartphones in both High school, and primary schools. Snapchat has been a major contributor to this surge in popularity.

These secure storage apps are being used to hide the evidence of sexting, sextortion, bullying and other inappropriate content that would normally be found when a phone is checked.

What is it?

There are several versions of these vaults around, but many masquerade as a calculator. They can be downloaded for free, by subscription or by an outright purchase. The more you pay the more secure and hidden your illicit content will be. Vault, Calc, Secret Vault are some examples. The storage capabilities vary. Calc in particular will store documents, images, films, links, downloads in a cloud.

How do they work?

Appearing as a calculator - the vault app requires a passcode to access the private stash of photo's that have been taken or sent. Some are so sneaky, that when the vault is discovered – a decoy passcode will lead to a relatively innocuous set of shots. Anyone searching could then stop at that point, unaware another passcode led to the real cache.

The calculator is functional, and the content is stored in a separate cloud that may be synced to an additional device/computer. Deleting the app may not be enough. The content is held elsewhere.

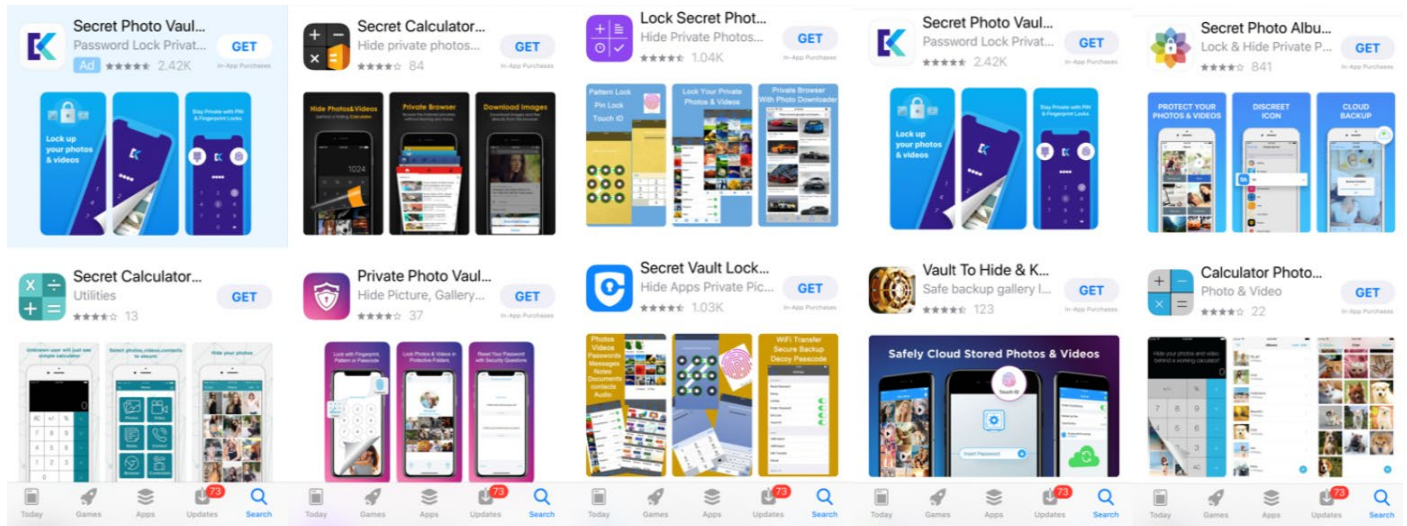
But wait there is more.

Those psychic moments your child has – when they somehow know you checked their phone? You may have had your mugshot taken. The app has the ability to take a photo of whoever was trying to access the vault with the wrong pin number. It then forwards this picture to the owner of the vault, and upgrades their security.

Private SMS applications

These applications allow for texts and phone call records to be hidden. Children and teens are easily able to hide interactions with individuals they have been warned to cease contacting.

The app pretends to be a legitimate messaging app but operates in the same way voicemail does – dialing in a pin number accesses the app. These apps are well hidden, not showing on the screen of device and when open – can be closed swiftly by a slight shake of the phone. There are similar versions that destroy communications from certain numbers regularly.



What can be done and what to look for?

- Look for duplicate apps. Two calculators, perhaps two messaging applications, If your teen has more than one application with the same purpose– there may be content they do not want you to see.
- Do some research. Have look on Google and the Apple store to see what is currently popular in vaults. You could spot some of these on your child's phone.
- Download one yourself and experiment with the features – this may make it easier to tell if your child is using this technology.
- Install parental controls on the App store and Google Play. A number of these vault application have an age recommendation of 17+, so you will be able to limit what your teen downloads by implementing parental controls.
- Talk to your child. These apps can hide a communication problem. The need to go to such lengths to keep part of their lives private can be a worrying sign. Bullying, being a bully, sexting and inappropriate images of minors that could result in child pornography charges are all things that can be hidden using these apps.

w: safeonsocial.com
e: wecanhelp@safeonsocial.com

No part of this e-book or its associated modules may be reproduced or transmitted by any person or entity in any form by any means, electronic or otherwise including photocopying, recording or scanning or by any information storage without prior permission other than the licensor who is licensed to use this information on their website, in newsletters and in print and has been granted permission from the publisher under an annual license.

The publisher, authors, licensee, licensor and their respective employees or agents will not accept responsibility for injuries or damage, physical or emotional occasioned to any person as a result of a social media use or any other activities described in this e-book.

Whilst every attempt has been made to ensure that the information in this e-book is accurate, it is the nature of social media to be constantly changing. Therefore, Safe on Social Media Pty Ltd gives no guarantees to the completeness or accuracy of the contents of this guide.